CHARTERGATES

SPECIALISTS IN TAX, VAT & EMPLOYMENT LAW

Chartergates Fact Sheet

SUBJECT: ACCOUNTABILITY

Underpinning the General Data Protection Regulation ('GDPR') are several data protection principles which ensure compliance in relation to the processing of an individual's personal data. These principles are broadly similar to the existing principles under the Data Protection Act 1998 ('DPA'). A significant change introduced by the GDPR is the new principle of accountability. This principle creates an onus on organisations to understand the risks that they create in relation to processing and to mitigate those risks.

What is the accountability principle?

The GDPR elevates the significance of accountability and expressly introduces the concept of accountability as an independent data protection principle. Article 5 (2) of the GDPR provides that '*the controller shall be responsible for, and be able to demonstrate, compliance with the principles.'* The GDPR explicitly places direct responsibility for compliance with the data protection principles on organisations processing personal data and further requires the organisations to **show** compliance in order to minimise the risk of breaches and upholds the protection of personal data.

How can you can show that you comply?

To comply with the principle of accountability, you should put in place comprehensive and appropriate governance measures. The appropriateness of measures will depend on the nature, scope, context and purposes of the relevant processing and taking into account the risk to the rights and freedoms of individual.

The Information Commissioner ('ICO') suggests implementing some of the following measures:

- ✓ Appointing a Data Protection Officer to monitor compliance, where appropriate;
- ✓ Implementing appropriate **technical and organisational measures** in relation to processing activities i.e.

    - ✓ internal data protection policies such as staff training;
    - ✓ internal audits of processing activities, and;
    - ✓ reviews of internal HR policies.

Any measures that are put in place will need to be periodically reviewed and updated, as appropriate.

- ✓ Maintaining **relevant documentation** on processing activities, in particular if organisations that employ more than 250 people are required to maintain internal records of data processing activities which are to be made available to supervisory authorities on request. If you have less than 250 you will be required to maintain records of higher risk processing activities;

| T: 01908 533255 | F: 01908 410333
| www.chartergates.com | Company No. 8203425
| Chartergate Legal Services Ltd, 5-6 Rankin House, Murdoch Court
Roebuck Way, Knowlhill, Milton Keynes MK5 8GB

- ✓ Implementing measures that meet the **principles of data protection by design and data protection by default** measures to show that the principles have been taken into account and incorporated into your activities, for example:

    - ✓ Data minimisation of personal data that is adequate, relevant and necessary;
    - ✓ Pseudonymising of data to reduce links with the identity of the individual;
    - ✓ Transparency;
    - ✓ Allowing individuals to monitor processing, and;
    - ✓ Creating and improving security features on an ongoing basis.

- ✓ Using **data protection impact assessments** ('DPIA') where an organisation uses new technologies or where the processing is likely to result in a high risk to the rights and freedoms of the individual.

You can also:

- ✓ adhere to **approved codes of conduct and/or certification schemes** to demonstrate compliance;

Of course, what is appropriate for your organisation will depend on the circumstances and it is important that businesses do not fall into the trap of just doing what everyone else does. We are able to assist you in determining what your specific needs are so that your compliance (and ability to show your compliance) is maximised.

Consequences of not complying with accountability

Failure to comply with the requirements of the GDPR and in particular, the accountability requirement, could result in a maximum fine of up to EUR 20 million or 4% of the organisation's worldwide annual revenue for the preceding financial year, whichever is higher. As the potential financial ramifications of non-compliance are substantial, we would advise ensuring full compliance with the GDPR

Now the GDPR is in force we would advise taking a systematic and proactive approach in preparation for the GDPR in relation to how you process personal data to demonstrate data protection compliance. It is essential to:

- ✓ review any existing policies and procedures to assess how the GDPR will affect your organisation;
- ✓ update any policies and procedures relating to the processing of personal data, and;
- ✓ implement appropriate measures to ensure compliance with the GDPR is adhered to.

Chartergates can help you navigate your way through your obligations under the GDPR to ensure full compliance. If you require any help or assistance, contact us now.